How to Set Up a Custom Login Page for Authentication

https://campus.barracuda.com/doc/4259897/

Setting up a custom login page for authentication is a three-step process:

- Create a Custom Login Page.
- Deploy the Custom Login Page.
- Configure the Barracuda Web Application Firewall to Use the Custom Login Page.

As an example setup, assume the following:

- A backend server at 192.168.128.10 needs access restricted to authenticated users. The particular web application resources that reside in "http://192.168.128.10/secure" require users to authenticate before gaining access.
- You want to authenticate users against an LDAP server.
- Service-1 (10.10.10.2:80) is configured on the Barracuda Web Application Firewall to secure access to the web application, with 192.168.128.10:80 configured as the server.

Step 1 - Create a Custom Login Page

Create a custom login page "login.html". It must contain the following:

- Form ID = nclogin
- Name = login
- Action = "/nclogin.submit"
- Method = POST
- User name field should be named - **f_username**
- Password field should be named - **f_passwd**
- An additional hidden parameter named **f_method** should be specified with value "LOGIN"

The form looks something like this:

```
<form id="nclogin" name="login" action="/nclogin.submit" method=POST>

    <p>User Name: <input TYPE="text" name="f_username">

    <p>Password: <input TYPE="password" name="f_passwd" >

     <p><input type=hidden name="f_method" value="LOGIN"><input TYPE="submit"
Value="Login"><input TYPE="reset" Value="Reset">
```

```
</form>
```

Step 2 - Deploy the Custom Login Page

You can deploy the custom login page either on your web server or on the Barracuda Web Application Firewall.

a. Deploying the Custom Login Page on the Web Server

Deploy the "login.html" file created in Step 1 - Creating a Custom Login Page on your web server. For example:

- The IP address of the web server is 192.168.128.10
- The “login.html” is available by accessing "http://192.168.128.10/login.html"

b. Deploying the Custom Login Page on the Barracuda Web Application Firewall

Create a custom login page on the Barracuda Web Application Firewall using **Add Response Page** under **ADVANCED > Libraries**. For more information, see Deploying the Custom Login Page on the Barracuda Web Application Firewall.

Step 3 - Configure the Barracuda Web Application Firewall to Use the Custom Login Page

After the custom page is deployed on your web server, configure the Barracuda Web Application Firewall to use the custom login page by doing the following steps:

1. Configure Authentication Service – Specify the authentication database server (LDAP) to use in order to authenticate user credentials. See How to Configure Authentication and Access Control (AAA).
2. Configure Authentication Policy – Create an authentication policy for the service you want to secure by clicking **Edit** next to the relevant service ("Service-1" in this example) on the **ACCESS CONTROL > Authentication** page.
3. In the **Edit Authentication Policy** window, configure the following:
    1. Set **Status** to **On**.
    2. Select *LDAP* from the Authentication Service drop-down list. Note that this is the authentication service created in Step 3.1.
    3. Enter your domain in **Session Cookie Domain**. For example: `www.example.com`.
    4. Specify values for other parameters appropriately and click **Add**. For more information,

click **Help** on that page.

4. Configure Authorization Policy – Create an authorization policy to specify the accessible resources after a successful authentication on the **ACCESS CONTROL > Authorization** page with the following steps:
    1. On the **ACCESS CONTROL > Authorization** page, in the **Add Authorization Policy** section, specify values for the following:
        - **Service** - Select the relevant service (Service-1 in the example) from the drop-down list.
        - **Policy Name** – Enter a name for the authorization policy. Example: `secure.access`
        - **URL Match** – Enter the URL of the secured part of the web application. In this example the URL is: /secure/
        - **Login Method** – Select HTML Form.
        - Click **Add**.

    2. On the **ACCESS CONTROL > Authorization** page, in the **Existing Authorization Policies** section, click **Edit** next to your new authorization policy (secure.access). In the **Edit Authorization Policy** window, do the following:
        - Set **Status** to **On**.
        - Specify “/login.html” in **Auth Not done URL**.
        - Set **Send Basic Authentication** to **Yes**.
        - Set **Send Domain in Basic Authentication** to **Yes** if you want the domain information of the client to be forwarded to the server along with the user credentials in the Basic Authentication Header. This is applicable only when **Send Basic Authentication** is set to **Yes**.
        - Specify values for other parameters appropriately and click **Save**. For more information click **Help** on that page.

After configured this way, when a client accesses "http://10.10.10.2/secure/mydoc.html", the client will be presented with the configured custom login page (login.html). The user ID and password forwarded by the web server custom login page are validated against the authentication server integrated with the Barracuda Web Application Firewall before the request is allowed to reach the backend web server.

If you enable Authorization for the entire website (/*), you must create a GLOBAL ACL rule with URL match set to the custom login URL (for example: /login.html) and the action **Allow**. Create this URL ACL rule on the **SECURITY POLICIES > Global ACLs** page for the associated policy to the service.

Note that a URL ACL rule created per website will not take precedence over the authorization policy.

Related Articles

Configuring Authentication and Access Control